IT Security

Application Security & SDLC

by Philipp Bandow

original slides by Bjoern Kimminich

Curriculum 2nd Semester

1. Open Web Application Security Project (OWASP)
2. Injection
3. XSS
4. Authentication Flaws
5. Authorization Flaws
6. Cryptographic Failures
7. Insecure Dependencies & Configuration
8. Software & Data Integrity Failures
9. Secure Development Lifecycle

Schedule

- **Tuesdays, 14:00 - 16:30**
- **Tuesdays, 14:00 - 17:15 starting from 13.09.22**
- 8 lectures (02.08. - 27.09.22)
- No lecture on 16.08.22
- 100% via ZOOM (invite distributed via email/calendar)

Test Exam

- **04.10.2022** (90min)
- **09:15 - 10:45** / Audimax
- ⚠️ Covers topics from both semesters
- ❎ Adjourning the exam is discouraged

System Requirements

To perform the exercises on your private computer you need

- *either* Node.js (18.x, 16.x or 14.x)
- *or* Docker

ℹ️ *On the university computers Node.js should already be available. You can verify this by running* `node -v` *on the command line. It should display a 14.x (or higher) version.*

💻 *You can always fall back to your personal laptop for the exercises as it should be free from virtualization, proxying or installation hurdles!*

Recommended Resources

- OWASP: OWASP Top 10 - 2021
- OWASP: OWASP Cheat Sheet Series

Literature Recommendations *(optional)*

- Kimminich: Pwning OWASP Juice Shop, 2022
- Stuttard, Pinto: The Web Application Hacker's Handbook 2, 2011
- Zalewski: The Tangled Web: A Guide to Securing Modern Web Applications, 2011
- Zalewski, Heiderich: Tangled Web - Der Security-Leitfaden für Webentwickler, 2012 (🇩🇪)

Awesome Web Security

> Curated list of Web Security materials and resources.

https://github.com/qazbnm456/awesome-web-security